УДК 681.322
Н.Н. Мошак, Е.А. Тимофеев. СПбГУТ, Санкт-Петербург, Россия

ОСОБЕННОСТИ ПОСТРОЕНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОКОММУНИКАЦИОННОЙ СЕТИ

Moshak N.N.,Timofeev E.A. PECULIARITIES OF FORMING INFOCOMMUNICATION NETWORK SECURITY POLICY

В последние годы в мире постоянно растет интерес к созданию инфокоммуникационных сетей (ИКС) общего пользования, создаваемых в соответствии с концепцией сети связи следующего поколения (Next Generation Network, NGN) [1, 2]. Это объясняется всевозрастающей ролью электросвязи в жизни современного общества XXI века, которое получило определение «Глобальное информационное общество».

Основная идея концепции ИКС заключается в объединении ресурсов информационных технологий и развитой инфраструктуры электросвязи с целью предоставления любому пользователю доступа к ним в реальном времени. Доступ к глобальным информационным ресурсам при этом реализуется посредством услуг связи нового типа, получивших название инфокоммуникационных услуг или услуг информационного общества. В сетях ИКС, помимо базовых услуг (контроль вызовов, идентификация, защита, биллинг), будут реализованы услуги по высокоскоростной передаче трафика различной природы с заданным качеством обслуживания (Quolity of Service, QoS), удаленному доступу к информационным базам данных, распределенной обработке данных, организации конференций и др. При этом сеть следующего поколения будет строиться на базе единых систем передачи и коммутации с предоставлением пользователю инфоуслуг на технологии «клиент-сервер» [1, 2]. Сеть ИКС предполагает также наличие объединенной автоматизированной системы эксплуатационно-технического обслуживания и административного управления.

Федеральная программа «Электронная Россия на 2002-2010 годы» [3] в рамках создания отечественной ИКС в ближайшие годы ставит задачи обеспечения населения минимумом инфокоммуникационных услуг, включающим в себя доступ к телефонной связи и сети Интернет в любом населенном пункте страны.

Помимо создания ИКС, другой не менее важной проблемой в глобальном информационном обществе является обеспечение информационной безопасности (ИБ), так как, например, только убытки от предпринимаемых вирусных атак на национальные информационные ресурсы в сети Интернет ежегодно составляют миллиарды долларов США [4]. Нормативным документом [5] информационная безопасность определяется как состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

В Доктрине информационной безопасности Российской Федерации [6] понятие «информационная безопасность» определяется как состояние защищенности национальных интересов в информационной сфере, включающее в себя защиту информационных ресурсов от несанкционированного доступа (НСД), а также обеспечение безопасности информационных и телекоммуникационных систем и рассматривается как одно из составляющих национальной безопасности.

Основные принципы построения политики информационной безопасности в ИКС изложены в [7]. Под политикой безопасности сети понимается формальная спецификация правил и рекомендаций, на основе которых пользователи используют, накапливают и распоряжаются информационными ресурсами и технологическими ценностями. Политика информационной безопасности в общем случае включают в себя:

- краткое описание объекта защиты;
- описание модели нарушителя;
- определение основных приоритетов ИБ;
- анализ информационных рисков;
- определение перечня и анализ значимых угроз ИБ на всех уровнях обработки, хранения и передачи информации в ИКС;
- описание требований к подсистеме ИБ.

Требования политики ИБ ИКС обеспечиваются на основе согласованного комплекса мер и средств, реализуемых соответствующей подсистемой, в том числе: административных и организационно-технических норм и регламентов, программно-технических средств защиты, а также регулярного мониторинга ее состояния.

Описание структуры ИКС. Базовым принципом концепции ИКС является разделение в сети функций переноса и коммутации информации от функций управления вызовом и функций управления инфокоммуникационными услугами.

Физическую структуру сети следующего поколения можно представить в виде объединения трех компонент: автоматизированных систем инфоуслуг (АСИ), мультисервисных или мультипротокольных сетей электросвязи (МСС) регионального и магистрального уровней, обеспечивающих услуги по интегральному переносу разнородного трафика в общей физической среде с заданным QoS, а также сигнальной и управляющей информации, и сетей широкополосного абонентского доступа (рис.1) [1, 2].

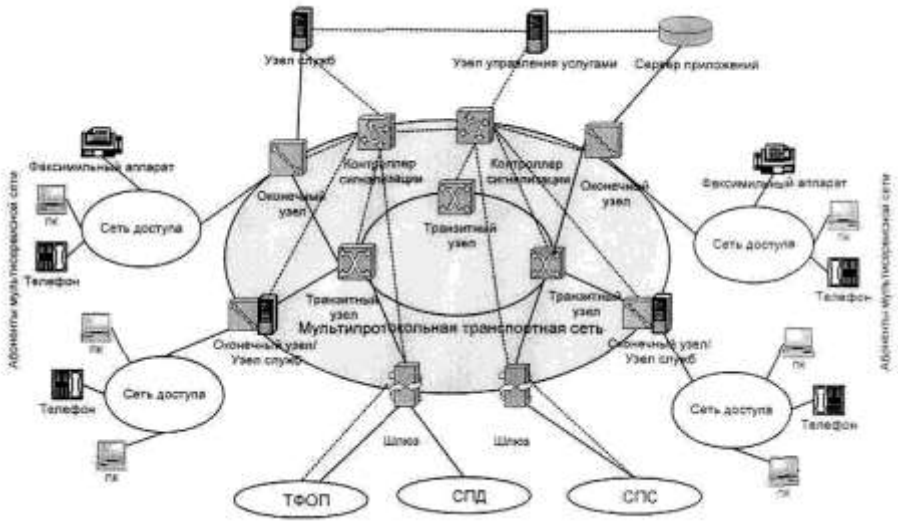

Рис. Структурная схема инфокоммуникационной сети

Основу АСИ ИКС составляют узлы служб (Service Node, SN) и узлы управления услугами сети (Service Control Point, SCP). Узлы служб SN играют роль серверов приложений, а узлы управления услугами сети SCP выполняют функции управления логикой и атрибутами услуг. При этом функции узлов служб SN могут также выполнять оконечные (оконечно-транзитные) узлы сети и системы Softswitch. Узлы и интеллектуальная периферия ИКС физически реализуются, как правило, на базе мощных компьютерных платформ, например серверов операционных систем (ОС) UNIX, системы управления базой данных (СУБД) Oracle и др.

В состав МСС ИКС могут входить:

- транзитные узлы, выполняющие функции переноса и коммутации;
- медиашлюзы (Media Gateway), позволяющие осуществить подключение к ИКС существующих сетей связи общего пользования и обеспечивающие транспортный сервис в сеансе связи;

- оконечные (граничные) узлы, обеспечивающие доступ пользователей к ИКС;
- гибкие коммутаторы Softswitch или «интеллектуальные» коммутаторы управления вызовами, поддерживающие основные группы протоколов сигнализации в ИКС: телефонной сигнализации (SS7), сигнализации пакетной телефонии (H.323, SIP) и управления медиашлюзами (MGSP, H.248) и выполняющие функции обработки сигнальных сообщений и управляющей информации;
- объединенная автоматизированная система (АС) эксплуатационно-технического обслуживания и административного управления;
- автоматизированная биллинговая система или автоматизированная система расчетов (АСР);
- подсистема ИБ и др.

В качестве технологической основы построения транспортной системы ИКС рассматриваются две пакетные технологии: технология асинхронного режима переноса ATM и технология протокола межсетевого взаимодействия IP [1].

Для организации широкополосного абонентского доступа пользователей к услугам ИКС используется:

- интегрированные широкополосные сети доступа, подключаемые к оконечным (граничным) узлам ИКС с возможностью предоставления пользователям выхода как в ИКС, так и в существующие сети общего пользования;
- существующие сети общего пользования, подключаемые к ИКС через медиашлюзы.

Описание модели нарушителя ИБ ИКС. Как уже отмечалось выше, построение политики безопасности для каждой компоненты ИКС должно исходить из описания ее модели потенциального нарушителя с учетом существования групп пользователей, обладающих различными полномочиями.

Сервисы ИКС относятся к сервисам высокого уровня, которые могут быть реализованы с использованием различных системных и прикладных платформ. Опишем потенциальную модель основных нарушителей для конкретных подсистем ИКС, реализованных на базе ОС UNIX и СУБД Oracle, или для случая, когда отдельные сервисы, предоставляемые оператором связи и/или поставщиком инфоуслуги, реализованы через доступ к базе данных на этих платформах. При этом необходимо иметь в виду, что действия нарушителей в сети ИКС могут проявляться не только в нарушении доступности услуг связи, но и в несанкционированном доступе к инфоуслугам или данным пользователей сети. Проанализируем так же возможные несанкционированные действия, которые они могут совершить в ИКС. Для анализа реальных угроз в различных подсистемах ИКС в качестве исходных могут быть использованы профили безопасности, разработанные на основе методологии национального стандарта ИСО/МЭК 15408-2002 и представленные на официальном сайте Гостехкомиссии России как нормативно-методический материал (http://www.gostexkom.ru). Профилем защиты (protection profile) называется (в соответствии с РД Гостехкомиссии России, 2003 г. «Руководство по разработке профилей защиты и заданий по безопасности») независимая от реализации совокупность требований безопасности для некоторой категории изделий информационной технологии, отвечающая специфическим запросам потребителя.

Привилегированный пользователь СУБД (администратор СУБД или нарушитель, несанкционированно получивший административные привилегии). Наибольшую опасность по возможности несанкционированных действий имеют системные администраторы СУБД Oracle, работающие под именами SYS и SYSTEM. СУБД Oracle построена так, что пользователи с указанными именами создаются при инсталляции СУБД (встроены в СУБД). Данная группа выполняет общесистемные функции по поддержанию работоспособности СУБД Oracle, а также некоторые работы по управлению прикладными БД, а именно: установка и запуск требуемого программного обеспечения сервера Oracle; установка прикладных БД, проведение их модификаций; создание резервных копий и восстановление

после сбоев системных и прикладных компонент; мониторинг работы прикладных БД, настройка производительности.

Администраторы СУБД с именами SYS и SYSTEM обладают неограниченными правами по манипуляции объектами прикладной БД. Необходимо отметить также, что в случае использования для контроля за действиями администраторов СУБД Oracle встроенных средств (журналов аудита), в силу архитектуры СУБД Oracle, администратор СУБД имеет неограниченные права по управлению содержимым журнала аудита, а действия администратора SYS вообще не регистрируются. Вследствие этого, ставится под сомнение возможность объективного и независимого контроля за действиями администратора СУБД в системе штатными средствами.

Деструктивные действия: несанкционированная настройка параметров СУБД, включая добавление и удаление учетных записей пользователей, присвоение привилегий пользователям, любые изменения данных, хранящихся в СУБД, а также хранимых процедур СУБД, нарушение безопасности СУБД и обрабатываемых данных.

Привилегированный пользователь прикладной БД (администратор БД или нарушитель, несанкционированно получивший административные привилегии). Как правило, администраторы БД занимаются разграничением прав доступа к объектам БД, ведением журналов регистрации работы в системе, выполнением регламентных операций в системе, требующих наличия повышенных полномочий. Администратор БД определяет права пользователей к объектам прикладной БД, осуществляет мониторинг их работы. Наличие указанных прав администратора БД создает потенциальную угрозу в части подмены (создания) пользователя АСИ с нужным администратору набором функций и задач для выполнения нелегальных действий от имени пользователя. Величина угрозы в данном случае будет определяться местом нелегального пользователя в технологической цепи обработки запроса в подсистеме ИКС, а также доступностью для него ключевой информации.

Отформатировано

Деструктивные действия: нарушение безопасности обрабатываемых данных прикладной задачи.

Привилегированный пользователь ОС Unix (администратор ОС или нарушитель, несанкционированно получивший административные привилегии ОС). Администратор ОС имеет все возможности по настройке параметров ОС, включая возможности добавления и удаления пользователей, присвоения привилегий пользователям, удаление журнала аудита ОС. Администратор ОС, не имея непосредственного доступа к информации БД, обеспечивает функционирование СУБД и прикладного ПО. Поэтому наиболее вероятными угрозами с его стороны могут быть разрушающие воздействия на программные средства АСИ и нарушение безопасности ОС и СУБД. Администратор ОС также имеет возможность бесконтрольного удаления записей журнала аудита ОС.

Деструктивные действия: несанкционированная настройка параметров ОС, добавление и удаление учетных записей пользователей, присвоение привилегий пользователям, удаление журнала аудита ОС (например, для trusted режима HP UNIX), нарушение безопасности ОС, СУБД и обрабатываемых данных прикладной задачи.

Привилегированный пользователь обслуживания аппаратной платформы приложения (администратор аппаратной платформы (АП) или нарушитель, несанкционированно получивший административные привилегии). Администратор АП владеет информацией об используемых физических устройствах и аппаратной конфигурации системы.

Деструктивные действия: внедрение в операционную среду программных «закладок».

Привилегированный пользователь системы информационной безопасности подсистем ИКС (администратор информационной безопасности (АИБ) или нарушитель, несанкционированно получивший административные привилегии). АИБ занимается управлением и конфигурированием систем защиты информации от НСД в подсистеме ИКС. Отвечает за обеспечение ее информационной безопасности, является экспертом в области используемых систем защиты информации от НСД, владеет информацией об аппаратной и программной конфигурации систем защиты.

Деструктивные действия: несанкционированная настройка систем защиты от НСД, систем криптографической защиты информации и предоставление несанкционированных полномочий в этих системах, изменение полномочий и списков доступа в системах защиты от НСД, что может привести к нарушению работоспособности компонент подсистемы ИКС.

Привилегированный пользователь активного сетевого оборудования транспортной системы ИКС (сетевой администратор или нарушитель, несанкционированно получивший административные привилегии в транспортной компоненте ИКС). Сетевой администратор владеет информацией об аппаратной и программной конфигурации сети.

Деструктивные действия: несанкционированная настройка таблиц коммутации и маршрутизации, изменение правил разграничения доступа на маршрутизаторах, перехват аутентификационной информации, нарушение функционирования мультипротокольной сети путем изменения маршрутной информации и правил контроля доступа.

Непривилегированный пользователь ИКС (пользователь сети).

Деструктивные действия: несанкционированное получение доступа к БД прикладных задач, без использования штатных средств АСИ или ТС ИКС с целью совершить в них несанкционированные действия .

Нарушитель, не являющийся пользователем ИКС.

Деструктивные действия: перехват служебного трафика ИКС с целью получения доступа к аутентификационной информации и формирование ложных SQL-запросов. Нарушитель может использовать так же сетевые средства по дезорганизации работы серверов ИКС и АРМ (зависания и/или перезагрузку).

Анализ значимых угроз ИБ ИКС и информационных рисков. Стандарт ISO 7498-2 [8] определяет пять базовых услуг для обеспечения безопасности компьютерных систем и сетей: конфиденциальность (confidentiality), аутентификация (authentication), целостность (integrity), контроль доступа (access control), причастность («неотпирательство», nonrepudiation), а также дополнительную услугу - доступность.

Сформулируем значимые угрозы нарушения услуг безопасности в ИКС.

Значимые угрозы нарушения ***доступности*** ресурсов:

- удаленные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки типа «отказ в обслуживании» (Denial of Service), использование возможных уязвимостей сервисов);
- локальные атаки на систему защиты ОС легальным пользователем (подбор паролей, использование возможных уязвимостей файловой системы, настроек сервисов и драйверов) с целью нарушения работы серверов приложений;
- неквалифицированные или неправомерные действия администраторов ОС и СУБД, приводящие к нарушению работы прикладных задач;
- изменения конфигурации ОС АРМ пользователей сети (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС и др.);
- удаление (модификации) исполняемых файлов прикладного и системного программного обеспечения;
- внесение компьютерных вирусов;
- внедрение программ, осуществляющих некорректные действия в АСИ, из-за имеющихся в них ошибок или специальных программных «закладок»;
- внесение модификаций в ПО, хранящееся на серверах ОС ЛВС системы управления сетью, приводящих к дезорганизации функционирования АРМ корпоративных пользователей;
- вывод из строя или изменение конфигурации сетевого оборудования, приводящее к потери доступа к сетевым ресурсам;
- удаленные атаки на средства защиты от НСД и средства криптографической защиты информации с целью нарушения их работы;
- неквалифицированные или неправомерные действия администраторов систем защиты информации, приводящие к нарушению работы этих систем.

Указанные действия приводят к нарушению доступности информационных, программных и аппаратных ресурсов, что в свою очередь ведет к дезорганизации процесса обработки информации в ИКС.

Значимые угрозы нарушения ***целостности*** программ и данных:

- несанкционированное изменение БД прикладных задач;
- несанкционированное изменение компонентов ОС и СУБД, а также программного обеспечения приложений;
- несанкционированное изменение операционной среды АРМ пользователей;
- несанкционированные действия нарушителя в АСИ ИКС от имени легального пользователя, носящие деструктивный характер или приводящие к искажению информации;
- изменения конфигурации и режимов функционирования файлового сервера ЛВС;
- внесение несанкционированных изменений в настройки коммуникационного оборудования.

Нарушение целостности хранимых и обрабатываемых данных, а также программных компонентов приложений, находящихся как на серверах узлов SN и/или SPC, так и на АРМ пользователей сети, может привести к некорректному функционированию программного обеспечения системы предоставления инфоуслуг и преодолению системы защиты. Кроме того, нарушитель, поразив целостность компонент ИКС, может заблокировать ее нормальное функционирование и тем самым осуществить атаку на доступность системы.

Значимые угрозы нарушения ***конфиденциальности***:

- ознакомление с конфиденциальными данными, хранимыми или обрабатываемыми в системе, лиц, не допущенных к данным сведениям;
- создание неучтенных, незаконных копий информационных массивов;
- хищение носителей информации (магнитных дисков, лент, запоминающих устройств и целых ПЭВМ;
- перехват административных паролей серверов и сетевого оборудования с помощью прослушивания сети;
- перехват IP-соединений и работа от имени администратора или пользователя;
- генерация фальшивых управляющих ICMP-пакетов для изменения параметров маршрутизации;
- использование слабых мест в сетевых службах для взлома сетевых ресурсов;
- использование слабых мест системы доменных имен DNS для формирования ложных таблиц хостов;
- использование протокола SNMP управления сетью для получения сведений о сетевом оборудовании и возможного перехвата и подмены управляющих сетевых сообщений;
- компрометация ключевой информации систем криптографической защиты информации и др.

Нарушение конфиденциальности может привести к разглашению или утечке информации и нанесению материального и морального ущерба юридическим или физическим лицам, обслуживаемым в зоне ответственности операторов ИКС. Кроме того, это может привести к несанкционированному получению привилегий пользователями СУБД или ОС и злоумышленному искажению ими информации БД, файлов аудита этих систем и др. Нарушитель, поразив конфиденциальность компонент ИКС(например, перехватив административные пароли) может также исказить конфигурационные файлы и тем самым осуществить атаку на целостность и доступность системы.

Значимые угрозы нарушения ***аутентификации***:

- компрометация ключевой и парольной информации систем аутентификации (в т. ч. нарушение конфиденциальности);
- создание неучтенных, незаконных account (входов) в систему;
- прослушивание сетевого трафика с целью перехвата незащищенной аутентификационной информации;

- перехват IP-соединений и работа от имени администратора или пользователя;
- перехват паролей за счет программных закладок (т. е. реализация угроз нарушения целостности программ и данных).

Значимые угрозы нарушения ***контроля доступа***:
- ошибки администрирования полномочий по доступу к ресурсам;
- ошибки реализации контроля доступа в операционных и прикладных системах и СЗИ.
- нарушение аутентификации.

Значимые угрозы нарушения ***причастности***:
- компрометация ключевой информации систем доказательства причастности (в т. ч. нарушение конфиденциальности);
- ошибки реализации криптографических алгоритмов систем доказательства причастности.

Особенности построения политики ИБ компонент ИКС. Проводя классификацию юридических и физических лиц, вступающих во взаимодействие между собой по поводу предоставления/получения инфокоммуникационных услуг, можно выделить следующие группы пользователей:
- пользователь – потребитель инфокоммуникационных услуг;
- поставщик услуги (Service Provider – SP) – индивидуальный предприниматель или юридическое лицо, оказывающее инфокоммуникационную услугу связи и не обладающее собственной инфраструктурой связи;
- оператор связи – предоставляет коммуникационные услуги (как пользователям, так и поставщикам услуг);
- поставщик информации (Content Provider - CP) – индивидуальный предприниматель или юридическое лицо, предоставляющее информацию поставщику услуги для ее распространения или предоставления пользователям по сети оператора связи.

Представители этих групп выступают владельцами различных частей аппаратных, программных и информационных ресурсов сети ИКС, рассматриваемой как единое целое. У каждого из них существуют свои интересы, своя сфера ответственности, и, соответственно, свои представления о реальных угрозах, связанных с информационной безопасностью. Естественно, что для каждой из компонент ИКС существует своя система приоритетов услуг безопасности, своя модель нарушителя (которая, как потенциальных нарушителей может рассматривать, в том числе, и представителей других групп) и необходимые меры защиты. При этом должны учитываться конкретные особенности организационных принципов построения ИКС, договорных отношений, на базе которых осуществляется взаимодействие сторон, участвующих в получении и предоставлении инфоуслуг, а также особенности эксплуатации технических средств и программного обеспечения ИКС.

Типичные угрозы для оператора связи МСС ИКС. Оператор связи, прежде всего, отвечает за доступность и конфиденциальность предоставляемых им коммуникационных услуг, работоспособность и сохранность оборудования сети и т. д. Поэтому политика ИБ оператора связи должна включать в себя требования по защите не только сетевых ресурсов и сервисов, перечень которых для IP-сетей достаточно хорошо описан в научной литературе (например, [9 - 11]), но и требования по защите собственных специализированных баз данных, используемых для управления сетью, в биллинговых системах [12] и др., сформулированные на основе анализа значимых угроз.

Для примера может быть рассмотрен перечень угроз биллинговой системы, которые должны быть проанализированы при формировании требований безопасности оператора связи [12]. Биллинговые системы предназначены для автоматизированного расчета с пользователями за услуги электросвязи и должны обеспечивать:
- точный расчет с пользователями за услуги электросвязи;
- защиту информации о пользователях услуг электросвязи;

- безопасное подключение операторов своей организации или организации - партнера по бизнесу;
- защиту информации, передаваемой по каналам связи внутри своей ЛВС.

Перечень угроз для билинговой системы, который должен быть положен в основу формирования требований ИБ, включает в себя:

- подмену адреса источника передаваемой информации с целью выдачи себя за уполномоченного пользователя (T.ADDRESS_SPOOFING);
- чтение, изменение (модификация), уничтожение значений параметров конфигурации системы (T.ATTACK_CONFIGURATION_DATA);
- обход реализованных механизмов защиты информации с целью получения доступа к системе или к защищаемым информационным ресурсам (T.ATTACK_POTENTIAL);
- потерю данных или переполнение журнала штатного аудита посредством создания определенного числа регистрируемых событий с целью сокрытия предпринятых нарушителем действий (T.AUDIT_FULL);
- воздействие на механизмы штатного аудита с целью вызова сбоя или отказа в работе данного механизма (T.AUDIT_UNDETECTED);
- осуществление НСД к программной и/или информационной части системы с целью доступа к передаваемой информации (T.BAD_ACCESS_UNAUTHORIZED);
- воздействие на механизм идентификации и аутентификации с целью получения доступа к системе, присвоения полномочий Администратора (T.BRUTE_FORCE);
- применение методов и средств криптографического анализа с целью получения доступа к программной и/или информационной части системы или осуществления НСД к передаваемой информации (T.CRYPTOGRAPHIC_ATTACK);
- осуществление физического доступа к системе с последующим целенаправленным нанесением повреждений или ее уничтожением (T.PHYSICAL_SECURITY);
- перехват и повторная передача данных идентификации и аутентификации с целью присвоение полномочий Администратора (T.REPLAY);
- перехват расчетной информации с целью передачи внешней системе (T.TRAFFIC_ANALYSIS);
- ошибки Администратора АС при настройке параметров конфигурации, нарушение Администратором АС технологии эксплуатации (T.CONFIGURATION);
- обмен информацией в обход билинговой системы (T.COVERT_CHANNELS);
- компрометацию используемых криптографических ключей (T.KEY_COMPROMISE);
- сбой и/или отказ отдельного компонента или всей системы в процессе ее функционирования.

Типовые решения для защиты каталога сетевых объектов мультипротокольной сети NGN, к объектам которого осуществляется доступ с использованием протокола LDAP, подробно рассматривается, например в [13]. Альтернативное решение по организации управления доступом к ресурсам сети на базе «клиент-серверной» технологии приведено в [14], где рассмотрены две системы подобного рода: NETRAC от TTI-TELECOM (СУБД Sybase) и TeMIP от COMPAQ (СУБД Oracle).

Необходимо отметить, что модель нарушителя, которая может приниматься во внимание при разработке политики ИБ в мультипротокольной сети, во многом зависит от характера деятельности оператора связи на рынке инфокоммуникационных услуг. При этом оператор связи должен обеспечить реализацию любой стратегии приоритетности услуг безопасности: целостность, конфиденциальность или доступность данных.

Типичные угрозы для поставщика инфоуслуг. В основе деятельности поставщика услуг, как правило, лежит предоставление доступа пользователям ИКС к базе данных, построенной с применением определенной СУБД. В связи с этим, на первый план у поставщика услуги выступает защита от НСД к информации на его серверах, целостность этой информации, а также целостность программного обеспечения, функционирующего на его серверах.

Отформатировано

Анализ защищенности информации в АСИ ИКС может быть рассмотрен на примере профиля защиты СУБД [15]. СУБД представляет собой приложение, использующее функции базовой системы (операционной системы хоста и/или сетевых сервисов, и/или специального программного обеспечения). Приложение СУБД может состоять из одного или нескольких выполняемых загрузочных модулей и одного или нескольких файлов данных. Данные БД могут постоянно находиться на одном сервере или могут быть распределены между многими независимыми серверами.

В этой связи политика АСИ должна строиться исходя из возможности осуществления угроз функционирования СУБД и операционной среды [15]:

- несанкционированный доступ к базе данных (T.ACCESS) нарушителя, который не является пользователем системы, или пользователя системы, который в настоящее время не является уполномоченным пользователем базы данных;
- несанкционированный доступ к информации (T.DATA). Нарушение разграничения внутри СУБД к объектам БД уполномоченным пользователем системы;
- чрезмерное использование ресурсов (T.RESOURCE). Угроза нарушения доступности информации в пределах СУБД. Пользователь базы данных выполняет действия, связанные с использованием чрезмерных ресурсов, периодически препятствуя законному доступу других пользователей базы данных к данным, ресурсам и сервисам;
- необнаруженное нападение (T.ATTACK). Угроза нарушения политики безопасности нарушителями с учетом контрмер, направленных на предотвращение других угроз;
- неправильное использование привилегий (T.ABUSE.USER). Ошибки (непреднамеренные или преднамеренные) уполномоченного пользователя в управлении доступом к объектам БД. Например, пользователь базы данных может предоставить доступ к объекту БД, ответственным за который он является, другому пользователю базы данных, способному использовать эту информацию для мошеннических целей;
- опасная операция (T.OPERATE). Компрометация базы данных может произойти из-за неправильной конфигурации, администрирования и/или функционирования системы;
- внезапные прерывания (T.CRASH). Внезапные прерывания функционирования СУБД могут приводить к потере или разрушению данных, связанных с безопасностью, таких как данные управления БД и/или данные аудита. Такие прерывания могут являться результатом ошибки оператора (см. также T.OPERATE), сбоев программного обеспечения, аппаратных средств, источников питания или носителей данных;
- физическое нападение (T.PHYSICAL). Критичные к безопасности части СУБД или базовой операционной системы и/или сетевых сервисов могут быть подвергнуты физическому нападению, которое может нарушить безопасность.

В [15], в соответствии с указанными выше угрозами, формулируются требования безопасности СУБД.

Отличительной особенностью базовых профилей безопасности, разработанных на основе методологии национального стандарта ИСО/МЭК 15408-2002, исходят, как правило, из предположения о наличии в составе персонала АС администратора, который единолично является ответственным за ее сопровождение, функционирование и контроль работоспособности. Например, для билинговой системы - это A.ADMIN и A.USER_TRUSTED [13], а для СУБД - A.MANAGE [15]. В указанном выше примере в основу построения политики ИБ АСИ положен аналогичный подход. Для управления АСИ и подсистемой информационной безопасности назначались одно или несколько доверенных лиц. В частности, предполагалось, что угроза T.ABUSE.USER не распространяется на пользователей БД с высоким уровнем доверия (предположение A.MANAGE).

Однако такое предположение не всегда оправдано. Во многих случаях (особенно это касается билинговых систем, а также АС эксплуатационно-технического обслуживания и административного управления ИКС) целесообразно создание выделенной службы безопасности и назначение администратора информационной безопасности (АИБ), который, не имея полномочий по управлению самой системой, осуществляет контроль процесса ее администрирования в части выполнения требований политики безопасности. При этом в

модели нарушителя в первую очередь необходимо рассматривать привилегированных пользователей, относящихся к техническому персоналу сети NGN [7]. Таким образом, возможен и другой подход к разработке политики ИБ АСИ, предполагающий разделение функций управления АСИ, с одной стороны, и контроля безопасности, с другой.

Типичные угрозы для потребителя инфоуслуг ИКС. Пользователем ИКС может выступать как отдельное физическое лицо, так и организация. Пользователя, прежде всего, интересует сохранность его компьютера (программной и аппаратной частей), целостность информации хранящейся на нем и, возможно, конфиденциальность информации передаваемой с использованием услуг NGN. Типичные угрозы для пользователя ИКС связаны, прежде всего, со следующими деструктивными действиями со стороны нарушителя:

- нарушение работоспособности ПО и аппаратной части компьютера (компьютеров, локальной сети), целостности информации компьютерах;
- кража информации с компьютера;
- потеря доступа к услугам сети;
- нарушением конфиденциальности передачи информации.

Основной путь реализации этих угроз – это распространение программ-«бомб» и программ вирусного характера, в том числе за счет подмены нарушителем серверов инфоуслуг.

Иерархия приоритетов услуг безопасности для пользователя зависит от характера его деятельности и ценности (значимости) информационных ресурсов, которая и определяет приоритеты их защиты.

Необходимо отметить, что для корпоративных пользователей инфоуслуг ИКС политики информационной безопасности должны разрабатываться с учетом их конкретной внутренней деятельности, включая требования по разграничению доступа легальных пользователей к внутренним ресурсам, ограничению их доступа к телекоммуникационным ресурсам ИКС и т. д. Однако эти вопросы требуют отдельного исследования и в данной статье не рассматриваются.

В случае если пользователь рассматривает сетевого оператора как потенциального нарушителя, он должен предусматривать также и требования к защите своего трафика.

Организация независимого мониторинга ИБ ИКС. Проведенный выше анализ позволяет сделать вывод, что основную опасность с точки зрения несанкционированного доступа к информации в ИКС и ее возможного искажения представляют собой действия лица, имеющего (или получившего путем преодоления средств защиты) наибольшие привилегии в любой подсистеме ИКС - привилегии администраторов баз данных, операционных систем и СУБД. При этом они могут скрыть свои деструктивные действия с помощью удаления полей штатных журналов аудита в силу наличия у них значительных полномочий с одной стороны, и невозможности обеспечения полного контроля их действий штатными средствами, - с другой. Например, в силу архитектуры СУБД Oracle, администратор СУБД имеет неограниченные права по управлению содержимым журнала аудита, а действия администратора SYS вообще не регистрируются в системе [7].

В этой связи мы приходим к выводу о необходимости внедрения в подсистемах ИБ ИКС независимых средств для контроля за действиями привилегированных пользователей, или так называемых доверенных средств мониторинга информационной безопасности [16]. Дополнительно, в случае если в функциональной структуре подсистемы ИКС имеется собственная служба информационной безопасности, то политика информационной безопасности должна содержать требования по разделению полномочий, а также реквизитов доступа (паролей) в подсистеме между администраторами сопровождения и администраторами информационной безопасности. При этом штатный аудит операционных систем, СУБД, БД и сетевого оборудования может быть использован для контроля действий администраторов со стороны АИБ.

Система внешнего (независимого) мониторинга представляет собой специально разработанные программные средства, основу которых составляют программные агенты

Отформатировано

(сенсоры), функционирующие на уровне драйверов соответствующих операционных систем. Необходимо отметить, что независимый мониторинг часто является единственным инструментом контроля привилегированных пользователей, а именно, в тех случаях, когда невозможно ограничить выполнение ими несанкционированных/деструктивных действий не лишив их при этом необходимой функциональности. Кроме того, для некоторых систем (например, ОС Novell NetWare) дополнительно все права по управлению штатным аудитом могут быть переданы независимому администратору.

Учитывая значительный объем данных аудита, поступающих от различных контролируемых подсистем ИКС, а также многообразие требований политики безопасности, которые должны быть отслежены через эти данные, становится очевидной необходимость автоматизации процесса их анализа. В настоящее время на мировом рынке уже появились системы указанного класса [16], производящие в режиме реального времени анализ, как данных штатного аудита различных систем, так и данных доверенного мониторинга на предмет соответствия определенному набору шаблонов, выражающих требования заданной политики безопасности. При этом в режиме реального времени на консоль АИБ поступают сигналы о тех или иных нарушениях. Кроме того, информация по всем событиям первичного (не разобранного) аудита и результатам анализа накапливается в базе данных, что позволяет производить последующие детальные расследования действий пользователей, в том числе с привлечением статистических методов. Особое значение имеет возможность совместного анализа данных аудита от различных подсистем, что позволяет с большей достоверностью выявлять подозрительные действия пользователей, в том числе распределенные атаки на систему.

Выводы

1. Политика информационной безопасности ИКС должна включать в себя отдельные политики безопасности ее кмпонент, модели нарушителей которых во многом зависят от характера деятельности операторов связи и поставщиков инфоуслуг.
2. При определении приоритетов услуг безопасности в моделях нарушителей в обязательном порядке должны быть учтены привилегированные легальные пользователи с правами администраторов компонент ИКС.
3. В состав ИКС должна входить система независимого мониторинга состояния информационной безопасности.

ЛИТЕРАТУРА

1. Концептуальные положения по построению мультисервисных сетей на ВСС России, Минсвязи России, 2001г.
2. Барабаш П.А., Воробъев С.П., Махровский О.В., Шибанов В.С. Мультисервисные сети кабельного телевидения / Под ред. В.С.Шибанова, СПб.: Наука, 2004. 404 с.
3. Федеральная программа «Электронная Россия на (2002-2010 годы)» // Электросвязь, №3, 2002.
4. Информационная безопасность как проблема глобализации инфокоммуникаций Материалы международного конгресса «Доверие и безопасность в информационном обществе» // Электросвязь, №6, 2003.
5. *Государственная техническая комиссия при Президенте Российской Федерации. Сборник руководящих документов по защите информации от несанкционированного доступа, М.: СИП РИА, 1998,120с.*
6. Доктрина информационной безопасности Российской Федерации // Новая газета. – 15 сентября 2000.
7. Н.Н.Мошак. Особенности построения политики информационной безопасности в мультисервисных сетях связи.IV Международный нучный семинар. Информационные сети, системы и технологии. Материалы семинара. –М., 2003. – 160 с.

8. ISO 7498-2. Basic Reference Model - Part 2: Security Architecture. - February 1989

9. В.Зима, А.Молдовян, Н.Молдовян, Безопасность глобальных сетевых технологий, -СПб.: БХВ-Петербург, 2000, 320с.

10. С.В.Запечников, Н.Г.Милославская, А.И.Толстой. Основы построения виртуальных частных сетей: Учеб.пособие для вузов. М.:Горячая линия-Телеком, 2003. – 349 с.

11. И.М.Гвоздев, В.Н.Зайчиков, Н.Н.Мошак, М.Б.Пеленицын, С.П.Селезнев, Д.А.Шепелявый. Отечественные средства для построения виртуальных частных сетей, Сети и системы связи, №12,1999, стр.10-20.

12. Билинговые системы. Защита от несанкционированного доступа к информации. http://www.gostexkom.ru

13. Василий Шабат. Каталоги LDAP и их применение, LAN, №3, 2003.

14. Дмитрий Гринько, Вадим Саякин. Управление гетерогенными сетями связи, LAN, №11, 2001.

15. Безопасность информационных технологий. Система управления базой данных. Профиль защиты 2002г. http://www.gostexkom.ru

16. Алексей Галатенко. Активный аудит. JetInfo №8 1999.

Н.Н. Мошак, Е.А. Тимофеев OTZI@lou.cbr.ru